快速通道

文档分类
- 红盟公告
- 新手上路
- 漏洞分析
- 工具介绍
- 安全配置
- 编程技术
- **安全技术** <=
- 业界动态

本类热门
- 如何利用黑客技术跟踪并分析一名目标人物
- 有关无线安全与黑客的话题
- 让我们回归(by 默难)
- 通用ShellCode深入剖析[转]
- Format String 漏洞介绍/总结(一)
- 结合实例解读ELF文件-阅读笔记(1)

有关无线安全与黑客的话题

提交文章： wking
提交日期： 2004-02-17
文章属性： 翻译
文档类别： 安全技术
浏览次数： 今4次/总8622次

==========有关无线安全与黑客的话题==========
[wking 译于03.8][bblman@21cn.com]

这是有关无线话题的最后一篇文章。[Just to remind you, the first article introduced the reader
to the Wireless world and discussed Wireless devices and protocols. The second article went
deeper into Wireless networks, provided general info on WLAN and discussed IEEE standards for
them.]本篇将介绍WLAN安全，说明一些最常见的攻击技术并介绍一些有用的工具。

概论
先简单介绍无线网络的扑拓。无线网络有两个主要的组成部件：基站和网络桥接器[stations (STA)and
access points(AP)].存在有[ad-hoc(peer-to-peer)and infrastructure mode]两种无线网络操作模式.在
[the ad-hoc mode]模式下客户端(STA)与客户端之间可以在网络内直接通信，无需透过Access Point。在
[the infrastructure mode]模式下客户端发送通信请求给总站，即[Access Point (AP)],它的作用就好比
网桥.该模式是种整合了有线与无线局域网络架构的应用模式。
一台装有无线网卡的客户端与网络桥接器(ap)间在传递数据前必须建立关系。一旦建立了关系它们将是
以下三种状态中的一种：

1.未授权和无关联。
2.授权但无关联。
3.授权并关联。

只有在第三种状态下信息交换才成为可能。届时网络桥接器(ap)以特定的频率发送标志管理帧。客户端收
到后，通过发送授权帧建立授权。授权成功后客户端又发送关联帧，最后网络桥接器(ap)回应关联。

无线网络安全机制
802.1标准为建立无线网络安全环境提供了一些机制。本段将为您介绍五种应用广泛的机制。

#连接对等协议[Wired Equivalent Protocol]

连接对等协议或WEP，首先被802.1标准的作者设计。那时WEP并不象IPSec协议一样用于

提供网络安全，而
是用于提供对等的保密级别。WEP的目标是通过加密无线电波来提供安全保证。WEP被用来阻止对无线网络的
非法存取。在外传数据已加密并打包的情况下WEP被缺省停用。

连接对等协议依赖共享于基本设置服务(Basic Set Service)上的密钥.该密钥在传输前加密数据包，并且
在它上面进行一次完整性检查。WEP使用的是一种流码名叫RC4算法。流码是将短钥扩充为无穷随机码的系统。

WEP加密算法

*尽管完整性算法提供了完整性检查值，比如我们所知的ICV,但纯文本消息仍在使用。802.11标准规定了
CRC-32的使用。
*在纯文本消息的最后附加了完整性检查值。
*24位的初始化向量(IV)产生其后连接着密钥。WEP的伪随机数生成器[pseudo-random number generator
(PRNG)]用它产生种子值。
*PRNG产生密钥序列。
*数据通过与密钥序列异或完成加密。
*暴露的IV被附加到保护帧(连同加密文本)并发送。
通过上面的条目，算法与解译过程可以被很容易地猜测。IV的作用是延长密钥的生存周期。WEP使用的是RC4密钥流，因此需要通过异或数据/ICV的联合体和24位IV,共64位key来产生它，密钥的长度为
40-bit.

#WEP 2

2001年在发现许多存在于最初WEP协议中的漏洞后，电子电气工程师协会(IEEE)建议修改WEP协议。新版本的
WEP2将IV的空间从24位增加到128位，并提供了Cerberus V的支持，但根本问题仍未被解决(这将在后面讨论)。
对全部WEP2的支持还有待于进一步的完善。

#开放系统认证[Open System Authentication]

每无线的网络有2个认证系统.开放系统认证是第一个并且是被802.11缺省的认证协议。从名字我们就可看出
该系统接受任何认证请求(比如空口令的root帐号)。WEP的无益体现在试验证明认证管理帧的暴露即使WEP已被
启动。

#访问控制列表[Access Control List]

在802.11标准中没有定义这种安全特征，但卖主用它提供额外附加的安全机制。访问控制列表基于客户的无
线网卡MAC地址(为每个NIC唯一确定)。网络桥接器(ap)通过ACL限制某些客户使用网络。若用户的MAC地址存在
于ACL则访问允许，否则，禁止。

#封闭的网络存取控制[Closed Network Access Control]

这一特征使得管理员可以选择使用开放式网络或封闭式网络。开放式网络意味着任何人都被允许加入网络，
而在封闭式网络，只有那些知道网络名或SSID的顾客才能加入。网络名就充当一把公钥。

无线网络攻击
你会发现本章节的内容更吸引人。它将介绍一些普通的用于破坏无线网络和盗窃带宽的攻击技术，确实很有
趣。如果你附近有无线网络或你居住的地区无线技术已被广泛地使用，下面描述的任何攻击技术将有98%的成
功率。

目前被攻击者盯上的无线网络有95%是完全无防卫的。当前的标准(802.11b)允许的带宽达11MBps。如果受攻
击的无线网络使用缺省设置值,则在带宽上将没有限制,它意味着攻击者能拥有完全的存取能力。在Neworder你
有一个很令人信服的例子- http://neworder.box.sk/newsread.php@newsid=3899

#桥接器电子欺骗与MAC地址嗅探[Access Point Spoofing & MAC Sniffing]

严密的身份认证手段使得存取控制列表列表[Access control list]提供合理的安全水平。但不幸地是MAC地
址并未幸免。攻击者可轻松地嗅到MAC地址因为它们肯定会被暴露即使当WEP被启用时。另外，无线网卡允许通
过软件更换MAC地址。一个攻击者能使用这些“ 特性 ”通过对网卡的编程伪装成有效的MAC地址，进入并享有网
络。

MAC地址的欺骗是很容易的。使用捕获包软件，攻击者能获得一个的有效的MAC地址包。如果无线网卡防火墙
允许改变MAC地址，那一切皆会发生。

如果一个攻击者有台无线设备，并且他/她在无线网络附近,他将能上演欺骗攻击。欺骗攻击中，攻击者必须
设置一个网络桥接器(AP),这里我们叫它“ 强盗 ”。它处于目标无线网络附近或在一个可被牺牲品信认的地点。
如果“ 强盗 ”的信号强于真实的网络桥接器(AP)的信号，受害者的计算机将会联接到攻击者的(Ap)中。一旦牺
牲品建立连接，攻击者就能偷窃他的口令，享有它的权限，设置后门等等。这种攻击主要用于获取口令。

#WEP攻击[WEP Attacks]

明文攻击

第一种情况：攻击者同时拥有明文本消息和其加密文本的拷贝。两者之间失去的部分便是密钥。为得到密钥，
攻击者将发送一数据到目标系统,同时又试图捕获那被送到目标系统的数据。一旦攻击者捕获到数据,他便得到
了IV。现在，他就能简单地运用字典攻击破解密钥。

另外在密文是通过明文与密钥流简单XOR形成的情况下。如攻击者拥有加密文本和明文,就能XOR已加密文本
从而获得密钥流。攻击者使用正确的IV和密钥流，可在没有被认证的情况下进入无线网络。

密文的再利用[Cipher stream Reuse]

该问题允许攻击者从一个WEP包(编码的包)复原密钥流。WEP的cipherment算法初始化向量时只声明了小空间，
通过溢出的方法发送各种各样的IV包,攻击者能捕获密钥流。之后,攻击者XOR明文本消息来解译密文(注意攻击
必须同时拥有密文本和明文本)。再以后，当认证数据在网络中传送时,攻击者能将它截取，并使用密钥认证数
据的明文。

Fluhrer-Mantin-Shamir Research

Cisco系统的Scott Fluhrer，以色列Weizmann研究所计算机科学部的Itsik Mantin和Adi Shamir在一年前着
手该项研究工程(2001年8月)。该项研究的目的在于解决RC4密钥排列算法[Key Scheduling Algorithm (KSA)]
的缺陷。
这个团体发现了KSA的两处缺陷。在他们研究论文中描述的攻击技术,既可以破解WEP(24位长)也可破解WEP2
(128位长)的密码。Adam Stubblefield或Rice大学、John Loannidis和AT&T实验室的Aviel Rubin也证实了这
一攻击技术。如此一来，2件新工具(air snort和WEPCrack)流传开来。但他们的源编码还未对外公布。

#Man-in-the-middle攻击

大多此类攻击都建立在毒害ARP或毒害缓存上。基本上，ARP欺骗是利用IP与以太网协议间相互作用的一种方
法。由于这篇文章不介绍ARP协议或ARP攻击，所以我将简略描述其攻击及其目的。

攻击者利用一个与目标网络具有相同类型的个人虚拟网络服务器结合access point,在用户试

图连接上真实
服务器时，伪装的服务器响应了它并将它连接向假冒的服务器。

考虑到这类的攻击在该篇文章中很难解释清楚，故向您推荐一些关于ARP的好文章在
http://www.ebcvg.com
/default.htm

#Low-Hanging Fruit

由于大多的无线网络是完全无防卫的(他们使用开系统认证)，且在缺省的情况下WEP不起作用，因此许多的
无线网络攻击者都以此方法作为开始。

一个攻击者所需的只是一块无线网卡和一台扫描仪(在文章的最后将有所解释)。攻击者扫描那些允许任何人
联入的开放式的access point，通过它攻击者们可得到免费的互连网使用权限，并能发动肉鸡攻击(攻击第三
方)等等。

无线网络的安全
由于无线网络使得雇员们在任何地点都能方便连入WLAN,因此无线网络在公司之间已经变得十分流行。但就
像其它新技术一样无线网络在安全方面的考虑是不够周到的。这节将描述一些最普通的改进无线网络安全的方
法。

#MAC地址过滤

这种方法将那些允许连入access point顾客的无线网卡的MAC地址列成一张表。如果存有多台access point，
则在所有的这些access point上列表都有效。管理人们应该时刻注意列表是否被更改。尽管这种方法不是很牢
靠(上面曾有谈到)，但在过去它是种广泛使用的无线网络保安方法。

#WEP

正如上面曾说的，WEP为顾客和access point之间的通讯提供数据编码的保护水平。值得一提的是WEP应该被
开启，因为没有必要为攻击行为大开方便之门。需再次提醒的是:WEP不是万能的，甚至在有些类型的攻击下它
很脆弱。

#SSID(Network ID)

为加强无线网络的安全，第一次的尝试是使用网络标识符(SSID)。当一位无线顾客想要与access point联系
时，SSID在这期间将被传播。SSID是被固定编入access point和客户端设备的一个7位字符。通过使用SSID,仅
有那些持有正确网络标识符的顾客才被允许与access point连接。在WEP启用后，SSID在传播中被从新编码,但
如果攻击者拥有与设备的物理连接，他/她将能获取以明文保存的SSID。

一旦SSID被某攻击者俘获，无线网络管理员人必须手工分配一个新的SSID。

#防火墙

使用防火墙来阻止对无线网络的非法存取可能是唯一的可靠手段。正如下面所提及的，对网络的存取需依靠
IPSec，secure shell或VPN。这样，防火墙应该被配置成只允许指定的IPSec或secure shell通信。下面将解释
从有线访问无线网络:

1.无线顾客端认证并与无线access point关联。为保证更好的安全,access point应被配置成可过滤MAC地址。

2.access point送一个请求给DHCP服务器。然后服务器为顾客分配网络地址。

3.一旦网络地址被分配，无线顾客便已进入无线网络。为能存取有线网络，它可建立一条IPSec VPN通道或使
用secure shell.

为防火墙进行安全配置十分重要，只有这样所有的非法联接才会被拒绝。

#网络桥接器[Access Points]

Access Points应该被配置成能过滤MAC地址,尽管MAC地址能被欺骗(看上面)。如果允许与它非法物理连接，
管理员们应确保AP被安置于一个安全的地方。

我们知道通过telnet或浏览器或简单网管协议可配置AP。但这里推荐只通过telnet并禁止其他所有别的途径。

#设计考虑[Design Considerations]

在实施任何加强无线网络安全的措施前，适当地计划十分重要。适当计划能排除与无线网络被联系后可能存
在的一些风险。
一些计划的要点：

1.用VPN或访问控制列表保护你的无线网络。

2.即使WEP被启用access point也不应该与内部的有线网络相连。

3.无论怎样access point都不应放置在防火墙之后。

4.无线客户应该通过secure shell,IP-Sec或virtual private network建立与网络的连接。这些方式提供了
用户授权，认证和编码等措施来加固你的网络安全。

相关链接

WEPCrack - http://www.ebcvg.com/download.php@id=1083
NetSumbler(windows) - http://www.ebcvg.com/download.php@id=1084
Airsnort - http://www.ebcvg.com/download.php@id=1085

Wireless Access Points and ARP Poisoning -
http://www.ebcvg.com/download.php@id=1158

Best Practices for Deploying Wireless LANs -
http://www.ebcvg.com/download.php@id=1160

Danny aka Dr.T (admin@ebcvg.com),
http://www.ebcvg.com/default.htm, July 2002
[wking 译于03.8]
[bblman@21cn.com]

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.
中国红客网络技术联盟 www.cnhonker.com
webmaster@cnhonker.net